IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

Renfinity, Inc., Plaintiff, v. Matthew Jones; MSD Enterprises, LLC; and Mil-Spec Engineering, LLC, Defendants.	**COMPLAINT** **(Jury Trial Demanded)**

NOW COMES Plaintiff, Renfinity, Inc. (hereinafter referred to by name or as "Plaintiff"), by and through counsel, complaining of Defendants Matthew Jones; MSD Enterprises, LLC; and Mil-Spec Engineering, LLC, and alleges as follows:

INTRODUCTION

1. It was all a ruse. Defendant entered into a contract to build an enterprise asset management application for Plaintiff to deploy and sell to other end users. The available evidence provides every reason to believe that Defendant never intended to honor that contract; rather, the supposed contractual relationship was nothing more than a portal through which Defendant could execute a lengthy fraudulent scheme designed to bilk Plaintiff out of as much money as possible – ultimately nearly half a million dollars. Defendant perpetrated the fraud primarily by repeatedly engaging in conduct that violates several federal criminal statutes, including the wire fraud statute and the witness tampering statute.

2. And Defendant's fraudulent scheme implicates federal interests in ways that go beyond simply having repeatedly committed several federal offenses. The fraud he committed involves lies and deception about projects being procured and developed by the Department of Homeland Security, Customs and Border Patrol. His fraud involves forging certain Homeland Security documents related to an "Authorization to Operate." His fraud involves forging fraudulent and inauthentic FBI Non-Disclosure Agreements and background check documents. His fraud involves creating false warnings and "notices" about the federal law enforcement consequences of disclosing certain information – all meant to do nothing more than silence those who may act as witnesses against his criminal conduct. The fraud was extensive and shows that Defendant Jones was willing to go to great lengths, including attempting to include other unwitting participants. It was white collar crime of the first order. And it bears repeating: Defendant conducted much of his fraud in ways that repeatedly violated federal criminal law – what the civil RICO statute refers to as a "pattern of racketeering." Plaintiff brings this action to recover all damages and other relief to which it is entitled.

JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1331, 1332. The federal claim is a civil RICO claim, and the parties are of completely diverse citizenship. To the extent that it may be necessary, the Court can also exercise jurisdiction under 28 U.S.C. § 1367.

4. This Court has personal jurisdiction over the Defendants. Defendants, acting through their agent, individual Defendant Matthew Jones, perpetrated a fraud that involved sending emails into the State of North Carolina to Jonnie Putney, Plaintiff's Chief Administrative Officer, whose office is in Huntersville, NC, in Mecklenburg County. These facts are sufficient to establish specific personal jurisdiction over Defendants related to the claims made herein.

5. Venue is proper in this Court under 28 U.S.C. § 1391(b)(1), (2), as the entity Defendants are subject to personal jurisdiction here for the reasons stated in the preceding paragraph and this district bears a substantial connection to this dispute for those same reasons.

PARTIES

6. Renfinity creates and offers "Secure Solutions for an Insecure World." Renfinity designs, manufactures and integrates cyber-secure common access protocols, asset management, wireless communication products and specialized industry solutions for enterprise organizations, its strength being specialized solutions that are highly integrated and scalable for asset management, access control and breach detection.

7. One of Renfinity's central products and offerings is its Secure Grid – its Enterprise Wireless Asset Management ("EWAM") System. Secure Grid is a scalable and flexible wireless Real Time Location System ("RTLS") network that enables enterprises to track and protect vital assets, people, equipment, and documents in real time. Secure Grid leverages both existing and Renfinity developed technologies

to provide an end-to-end solution that can scale to meet the needs of any business or enterprise. The components of the Secure Grid system include:

a. Industry Standard Radio Frequency Identification ("RFID") Tags

b. RFID Repeaters (Exciters)

c. RFID Readers

d. Secure Grid Data Gateways

e. Secure Grid Data Collection Software

f. Secure Grid Connection Profiles and API's

g. Renfinity Hosting and Professional Services

8. Renfinity's cyber-secure, wireless network infrastructure is scalable, integrated, portable, mobile, automatically meshing, self-healing system that is fully compliant with Federal Information Processing Standards ("FIPS"), including FIPS 140-2: Security Requirements for Cryptographic Modules; FIPS-197: Advanced Encryption Standards; and FIPS-201-2: Personal Identity Verification (PIV) of Federal Employees and Contractors.

9. By way of further example, the Secure Grid Visitor Management features, to take one component of the system, ensure that customers' staff and visitors are safe and protected while in the customers' facilities, by providing the following:

a. Cyber-secure monitoring of real-time movement transactions (FIPS 140)

b. Monitor visitor's movements and activities in real-time

c. Access Control for escorts and visitors

d. Geo-Fencing for visitor access and common areas

e. Real-time alerts for unescorted, tailgating and breach detection for visitors

f. Facial recognition for stranger alerts

g. Active Shooter alerts and enterprise-wide notifications

h. Automated security procedures

i. Enterprise video, intercom and facial recognition integrations

j. Integrates securely with existing visitor management solutions

k. Protect staff, visitors, patients, students, assets, etc. from strangers and breaches

10. According to documents and information provided by Defendant Matthew Jones, Defendant MSD Enterprises, LLC is a Texas entity. A search of the Texas Secretary of State website prior to initiation of this action, however, revealed no evidence that MSD Enterprises, LLC ever existed in that State. On information and belief, no such corporate entity was ever formed in Texas, and MSD is in effect a sole proprietorship for which Defendant Jones is the owner and responsible party.

11. According to documents and information provided by Defendant Matthew Jones, Defendant Mil-Spec Engineering, LLC is a Texas entity. A search of the Texas Secretary of State website prior to initiation of this action, however, revealed no evidence that a Mil-Spec Engineering, LLC ever existed in that State. On information and belief, no such corporate entity was ever formed in Texas, and

Mil-Spec is in effect a sole proprietorship for which Defendant Jones is the owner and responsible party.

12. Defendant Matthew Jones is, on information and belief, a citizen and resident of some State other than North Carolina. Based on the best information currently available, Defendant Jones is a citizen and resident of either Virginia or Texas. Because Plaintiff has been unable to confirm the actual existence of the entity Defendants, and because Defendant Jones was acting as their agent at all relevant times at any rate, references to "Defendant Jones" should hereinafter be understood to refer to all Defendants.

FACTS

13. In or around April of 2014, Renfinity engaged Defendant Jones to assist in the development of software and hardware for Renfinity's Secure Grid product. Plaintiff's founder (Renee McCown) and Defendant Jones had collaborated on the development of a similar app previously while each was working for earlier employers.

14. Renfinity would later learn that the app that Defendant Jones was "selling" and "developing" – while it was supposed to be developed for Plaintiff's exclusive ownership and control – was actually developed and owned entirely by another company. Defendant Jones played no part in the development of the app, owned no rights to it, and was ultimately unable to deliver it to Plaintiff despite Plaintiff having paid substantial amounts of money for the development. Yet Defendant Jones consistently misrepresented the status of the development and came

up with various ways to apply pressure for Plaintiff to send funding for the project, and was thus able to defraud Plaintiff out of nearly half a million dollars.

15. Before Renfinity engaged Defendants to develop the subject app, and throughout the time period during which that development was supposed to be taking place, Renfinity solicited and secured many investors to help fund the project, and was able to do so in large part based on material misinformation Defendant Jones repeatedly submitted over the course of the interactions between the parties. Renfinity itself did not know that Defendants were engaged in such a fraud and had no reason to know. Defendant Jones actively concealed the fraud on an ongoing basis. Renfinity's investors stand to potentially lose large of sums of money if Defendants are not held to account for the wrongdoing set out herein.

16. In mid-April of 2014, the parties detailed their engagement in a Statement of Work provided by Defendant Jones. Secure Grid was based upon the previous development of a similar application the Defendant had developed previously in or around 2010.

17. Pursuant to the Statement of Work, Defendant Jones was to develop the Secure Grid software, conduct testing and evaluate the performance of the system through a pilot test, and provide the Secure Grid SLED (a carrier case for insertion of access cards to allow for tracking of assets) and certain drone technologies in a packaged system, which was to be provided to the Department of Homeland Security/Customs and Border Patrol ("CBP"), as well as other end customers.

18. In retrospect, Defendant wasted little time in beginning to pressure Plaintiff for funds. Shortly after the Statement of Work was circulated, Defendant informed Plaintiff that unless Plaintiff was able to come up with funding for the project, the solution would be sold to another bidder.

19. Plaintiff promptly provided Defendant with funding confirmation for the down payment of $95,000 and subsequently wired that money to Defendant to secure the contract. That down payment was supposed to allow Defendant to begin development of Plaintiff's application.

20. Several months later, having secured the down payment from Plaintiff but not yet the balance of the contract price, Defendant came to Plaintiff with what was sure to be an exciting new opportunity. Defendant reported that the Customs Border Patrol (CBP), an Agency of the Department of Homeland Security, wanted to use Plaintiff's application for a pilot program for a secure southwest border project. Presenting this new "opportunity" to Plaintiff allowed Defendant to press Plaintiff for further payments on the development contract.

21. Plaintiff secured the necessary investors to capitalize on this newly divulged "opportunity" that Defendant Jones presented. In or around January of 2015, Plaintiff arranged for Defendant Jones to make a pitch to certain investors, who subsequently wired a $100,000.00 investment to secure the parties' ability to participate in the CBP project.

22. Several weeks later, Defendant provided a briefing to Plaintiff and the investors, stating that he was in the process of developing the application and

providing supposed details, an exercise that he repeated several weeks later. In fact, Defendant never developed Plaintiff's application and never did anything more than make numerous material misrepresentations to lead Plaintiff to believe that the product was in development.

23. A few weeks later, Defendant upped the ante a bit. He provided an update on the purported progress with the CBP pilot program and forwarded information that he presented as having been supplied by the Department of Homeland Security (DHS). Defendant Jones also provided information about the site for the CBP Secure Grid pilot – a project that he stated was being undertaken in conjunction with a Native American owned contractor named Suh'dutsing pursuant to a Teaming Agreement. He would eventually provide an actual copy of the purported Teaming Agreement, but Plaintiff was later able to confirm with the contractor that it was a false and fraudulent document.

24. In the months that followed, Defendant Jones continued the fabrications and kept up the appearance that all was well and running according to plan. In or around July of 2015, for example, he provided Plaintiff with the CBP brief, which included Renfinity's Secure Grid solutions; several months later, he provided an email showing his company as the manufacturer for Plaintiff's products; he emailed Plaintiff about the cost of the video demonstration that was to be to be provided to investors; he provided Plaintiff with an outline of the Secure Grid's solution features and functions in preparation for his presentation to Plaintiff and the investors.

25. On November 29 of 2015, Defendant actually stood before Plaintiff's agents, employees, and investors and made a complete presentation about Secure Grid as if he and his company were the ones developing it. Stafford Mahfouz, an employee of Johnson Controls, Inc., joined Defendant Jones in making the presentation; Mr. Mahfouz later acknowledged that Defendant Jones told him to lie about the product; the product being presented that day was not Plaintiff's application that Defendant Jones was developing for Plaintiff. The product was in fact owned and developed for an entirely different company by someone other than Defendant Jones. He literally played no role in developing it and presented it as if it were the product he was developing and had developed for Plaintiff. According to Mr. Mahfouz, Defendant Jones told Mr. Mahfouz that the investors couldn't know the truth because Renee McCown didn't want the investors to know the truth. Mrs. McCown said nothing of the sort and had no reason to lie to or mislead Renfinity's investors.

26. A few months of relative silence followed, as Defendant was purportedly working on the development of the Secure Grid app. On or about September 23, 2016, in a further effort to make the entire undertaking look legitimate, Defendant actually created a purchase order for the Plaintiff's Secure Grid application. Pursuant to that purchase order, Defendant would pay Plaintiff $650,000 if the Secure Grid pilot was successful.

27. After a few more months of relative silence while Defendant was purportedly working on development of the Secure Grid app Defendant sent an

updated purchase order in early February of 2017. Under that purchase order, Defendant would pay Plaintiff Renfinity $1,389,750.00 upon completion of the pilot program, which Defendant Jones reported was then underway.

28. A few days later, Defendant emailed the purported deployment plan for the CBP pilot for both the Defendant's application, REDCO, and the Plaintiff's application, Secure Grid, and then provided a new purchase order for Plaintiff's Secure Grid/ Smart Card (SLED).

29. In late February of 2017, Defendant Jones made a presentation about his company's purported Teaming Agreement with Suh'dutsing for the CBP pilot project – the same Teaming Agreement that Suh'dutsing would later confirm was a forgery. No such agreement existed between Suh'dutsing and Defendant Jones or any of his companies; but Defendant was keen to cover his tracks and conceal his fraud at all times.

30. That same month, Defendant broached the possibility of other new projects for Plaintiff's Secure Grid application. Specifically, Defendant requested information to begin costing Secure Grid for the Port of Charleston with Johnson Control Systems. Defendant concealed the fact that he was not a JCI reseller. Defendant needed to be a JCI reseller in order to fulfill his contractual obligations to Plaintiff.

31. The following month, in mid-March of 2017, Defendant Jones returned to using the other existing "opportunities" to squeeze more money out of Plaintiff. He sent Plaintiff an email for the purported purpose of providing updates from the CBP

for the SLED. Defendant Jones requested payment of $120,000 for the SLED upgrade. He tried to create a false sense of urgency in his email, stating that "[t]o move from hold to scheduling we are required to submit a deposit of $20,000 of the $100,000. Because of previous delays and start and stop on projects MSD can not burn the relationship with RSDU and advise other than the real-time status."

32. Plaintiff sent the $20,000 and Defendant acknowledged receipt in an email. Around that same time, Defendant Jones provided a brief on Plaintiff's Secure Grid Smart Card (SLED) design – again trying to create or keep up the impression that he was actually working and making progress on the various obligations he purportedly undertook to Plaintiff.

33. The following month, in April of 2017, Defendant pushed onward. He provided a design of Plaintiff's Secure Grid Smart Card (SLED) design and stated that the SLED manufacturer would provide previous SLED prototypes that were not operating according to specs. All's well on the home front – or so Defendant Jones would have Plaintiff believe. Defendant sought to create the impression that the projects were running along with nothing more than the typical hiccups that one might expect.

34. It was around this time that Defendant Jones reported to Renfinity that he and his company would be entering into a Teaming Agreement with Suh'dutsing Technologies, Inc. for the live, on-site demonstration of the system for the CBP pilot program. Not content to stick with the current scope of that project, Defendant Jones reported to Renfinity that CBP was requiring that drone technology be part of the

system to be purchased; of course, Defendant Jones presented Plaintiff with an invoice for that technology. But Defendant Jones never delivered that technology to Plaintiff despite Plaintiff having paid for it.

35. Turning back to the as yet underdeveloped opportunities for his fraud, Defendant Jones provided Plaintiff with an update for Port of Charleston Pilot Cost sometime in or around May of 2017. Specifically, Defendant supplied the following schedule:

a. Start Date: 5/22;

b. Balance Due $20,000 6/26;

c. Beta Run (10): ~$6,500;

d. Production Tooling: ~$37,000;

e. Production Board Run (100): ~$20,000;

f. Production Enclosure (100): ~$3,000.

36. Defendant Jones followed this communication with another email sent on or about June 20, 2017, requesting $45,000 because the "CBP capabilities demonstration is on the week of 7/17. This may require ~$45,000 of the $200,000 we advised to set aside for the contract in case we needed to accelerate any equipment orders. I'll know more at the end of the week."

37. In the meantime, Defendant Jones continued to indicate that the other projects were running fine. On or about June 29, 2017, for example, he provided Defendant's schedule for SLED development and delivery. None of this was true. He was not in fact developing the projects as promised, never had any intent of ever doing

so, and has never been able to deliver any of the products or solutions that Plaintiff paid him to develop.

38. On or about June 30, 2017, Defendant followed up with another request for $45,000 for CBP Demonstration capabilities. Attempting to create yet another false sense of urgency, Defendant stated on a phone call that failure to provide funding put Plaintiff at risk of losing entire pilot project.

39. On or about August 9, 2017, Defendant delivered a PO for REDCO Demo and Development Invoice for $45,000, claiming that funds were required to demonstrate the CBP capabilities on the week of 7/17. "This may require ~$45,000 of the $200,000 we advised to set aside for the contract in case we needed to accelerate any equipment orders." Of course, we know this was false and was intended to deceive. There was no Teaming Agreement and no CBP project for Defendant Jones or his companies.

40. On or about September 12, 2017, Defendant supplied the updated schedule for the Plaintiffs' Smart Card (Sled) and information regarding the CBP Pilot. According to Defendant Jones, it was necessary to implement a corrective action plan. Defendant stated that the schedule was as follows: Current board "alpha" rework – COMPLETE; Revision testing and modifications – COMPLETE; Enclosure design from final "alpha" design – COMPLETE; Enclosure and battery integration and testing - October 2 - October 23; Operational Software and API modifications - October 16 - November 20; Integration testing with Secure Grid

Platform and modifications - November 20 - December 11; Complete customization of the Secure Grid Platform with the SLED integrations - December 11 - January 22

41. By October of 2017, time was catching up with Defendant Jones, as, at some point, he was going to have to explain why no products or services were being delivered and why no payments were being received or revenue generated for Renfinity. It is in light of that reality that, on or about October 6, 2017, Defendant Jones sent an email explaining a purported delay in the CBP Pilot. He created an entirely fabricated story about certain defects in the test runs of the system and went so far as to create and attach to the email an elaborate Corrective Action Plan that, according to Defendant, had been or was being submitted to CBP.

42. Specifically, the Corrective Action Plan, which was nothing more than an entirely bogus effort to suggest that there was a legitimate reason for the delay in payment and revenue generation and buy Defendant more time, stated that there had been "*[t]echnical failure of ground radar system that was used under the request of CBP. The radar failed due to the 6 degree azimuth and above ground level (AGL) of the equipment at 80'. This failure caused a 30 day delay in testing and demonstration. I was given a template to use from CBP to identify the deficiency and what corrective action would be taken. The document submitted to my POC at CBP is attached. We have identified, tested and integrated the radar system from FLIR and got approval from CBP. We are scheduled to complete final testing at the end of October. This would also push the project completion NLT the end of Q1 FY18 (December is when we expect*

payment)". None of this was true and was an attempt to do little more than continue to conceal the active and extensive fraud being perpetrated by Defendant Jones.

43. With little other choice than to continue the cover up, Defendant Jones sent Renfinity an email on or about October 27, 2017 stating that he was preparing for the final review meeting and capabilities demonstration for authorization to proceed with the CBP project. He would later provide Plaintiff with a forged and fraudulent document purporting to be an Authorization to Operate allegedly issued by Homeland Security for Plaintiff's application and solution to be used on the CBP site.

44. Meanwhile, the same month that Defendant was continuing the farce that he was actively developing Plaintiff's application and taking every conceivable step to conceal his lies with more lies (October of 2017), Defendant Jones was sure to give Plaintiff his updated banking information so that he could continue to receive the wire transfers from Plaintiff – followed shortly thereafter with a cost breakdown for implementing the bogus Corrective Action Plan for the CBP pilot.

45. In the meantime, Defendant had to continue to cover up the lie he told about the alleged Teaming Agreement. Plaintiff had expressed interest in viewing that agreement, which is a request for which Defendant had not planned. Thus, on October 27, 2017, Defendant Jones sent Plaintiff an email stating that he would "send the subcontract agreement over as soon as I can." But it didn't stop there. Defendant, needing to leave himself room to continue the cover up, stated that he would contact the contractor "to have legal submit what can be released." He closed with the false

notion that he'd be spending the weekend preparing for the final review meeting with CBP.

46. As previously noted, Defendant's modus operandi was to attempt to shroud the projects with an air of secrecy imposed by external legal constraints because of the allegedly sensitive nature of the projects from a national security perspective. This was, after all, a border protection project being procured by the CBP. Thus, legal needs to review it to see what can be released. And, ever the creative criminal, when Defendant Jones got around to forwarding a copy of the purported agreement to Plaintiff by email dated November 2, 2017, the sole content of his forwarding email was the following "NOTICE:"

> THE INFORMATION ATTACHED HAS BEEN DEEMED LAW ENFORCEMENT SENSITIVE AND THE RELEASE OF ANY INFORMNATION RELATED TO THE INFORMATION ATTACHED OUTSIDE THE SCOPE OF THE EXISTING MSD AND RENFINITY NDA IS STRICTLY PROHIBITED WITHOUT THE PRIOR WRITTEN APPROVAL OF MSD AND THE US GOVERNMENT. CONSEQUENCES OF SUCH BREECH COULD RESULT IN FINES UP TO $250,000 AND POSSIBLE IMPRISONMENT.

47. Aside from the bad grammar and misspelling of the word "breech," the purpose of this supposed disclaimer or "NOTICE" is patent. The Teaming Agreement was a fraud; Defendant Jones knew it was a fraud; and he's trying to use a fabricated threat of legal sanction to scare Renfinity out of telling anyone about what's going on.

48. A little over a month later, the fraudulent emails – and thus the substantial pattern of racketeering activity – continued. On or about December 11, 2017, Defendant Jones sent another status update on the CBP project. That email continued to perpetrate the falsehood that he was working with Suh'dutsing to

develop the CBP pilot and that everything was in order pursuant to schedule. According to this most recent status email, Plaintiff could expect to get paid on the CBP pilot project no later than about March 9, 2018 – thus buying Defendant a few more months of time on his fraud scheme.

49. In the meantime, Defendant had provided Plaintiff with yet another fraudulent document. Specifically, on or about December 6, 2017, Defendant Jones sent a fabricated "Authorization to Operate" purporting to signify that Homeland Security had accepted Plaintiff's application and solution for the CBP project. Defendant stated that divulging the contents of this document was a violation of national security for Plaintiff and Defendant – which of course is not true and was not intended to do anything other than keep Plaintiff quiet about matters that might lead to the discovery of Defendant's fraud. Defendant also threatened to "shoot any one at Plaintiff's organization who divulged this information." Defendant was serious about concealing the fraud.

50. In early January of 2018, Defendant Jones acknowledged receipt of the most recent wire transfer and that he had, after that, been paid in full for the CBP project. He then repeated the falsehood that Plaintiff could expect to receive its money for the CBP purchase order ($1.38M) by March 9.

51. With his ability to defraud Plaintiff on the CBP now effectively terminated by his acknowledgement of payment in full, Defendant had no choice but to turn back to the other ongoing "projects." Thus, on or about January 22, 2018, Defendant Jones invoiced Plaintiff' for the Port of Charleston project in the amount

of $37,147.00. Plaintiff rejected that invoice due to the fact that Defendant had not performed processes required to assess the cost. A few days later, Defendant Jones, oddly enough, actually requested that the invoice be cancelled, and Plaintiff obliged. Not to be so easily thwarted, however, Defendant immediately followed up with a request to be reimbursed for equipment purchases: "Jonnie, attached is the equipment invoice for the Port of Charleston pilot. The equipment has been purchased and Renee asked to send the invoice for payment." On information and belief, Defendant Jones did not purchase the subject equipment and was not entitled to reimbursement of the claimed equipment expenses.

52. About a month later, Defendant Jones came up with a new reason to submit an invoice to Plaintiff. As the forwarding email stated: "Renee attached is an invoice for C-Cure 9000 equipment needed to test SLED interface with C-Cure equipment. This is the access control that the federal government uses and will be used in Charleston. I need to get this out ASAP to avoid delays for SLED interface testing and assurance."

53. By now, Defendant's emails are becoming a bit too predictable and routine. His suggestion that he needed to get the situation resolved "ASAP" is his old familiar tactic of attempting to create a false sense of urgency. Plaintiff rejected this invoice because it had already paid for the subject services as part of an earlier invoice. Thus, in his desperation to defraud Plaintiff out of substantial sums of money, Defendant Jones had forgotten that he had already invoiced Plaintiff for certain services (or maybe just didn't think Plaintiff would review the invoice closely

enough to catch it) and he resorted to double billing for the same services previously billed and paid for.

54. In the months that followed, Defendant Jones continued to spin out his tales and fabrications. On or about February 26, 2018, he sent several materially false and fraudulent emails related to the Port of Charleston (POC), followed shortly thereafter by an email on or about March 2, 2018, perpetuating the falsehood that Plaintiff would receive payment on the CBP purchase order on March 9, 2018.

55. Toward the end of March in 2018, Defendant again showed how far he was willing to go in an effort to cover up his fraud. Specifically, on or about March 27, 2018, Defendant Jones effectively plagiarized and falsified FBI Non-disclosure Agreements and background check materials and tried to get all of Plaintiff's employees to execute those documents. When Plaintiff – unaware of Defendant's duplicity and taking national security concerns seriously – presented the FBI documents to the Port of Charleston to get the NDAs signed and executed, the POC informed Plaintiff that the documents were inauthentic. These documents were reported to the FBI at the POC and later shown to the FBI in Charlotte, who confirmed the documents were not valid.

56. With time running out on his CBP and POC fraud schemes, Defendant needed a new potential customer or project for Plaintiff to provide products or services to. On or about April 9, 2018, Defendant notified Plaintiff of a good business opportunity with a potential customer who may want to use some of Plaintiff's products or services. Defendant provided the name of the person, the name of the

business, and the contact information for this new potential customer to Plaintiff. Nothing came of this information, but it was certainly an effort to open a door that Defendant Jones could exploit to extend his fraudulent scheme.

57. With Defendant's latest salvo going nowhere, Defendant was running out of time. With little to no additional fraudulent funds coming in, and having delivered none of the promised products, Defendant Jones had to continue to try to think up explanations. Thus, on or about April 22, 2018, he sent Plaintiff an email stating that the SLED would not be delivered as ordered because of the invoices that Plaintiff had rejected earlier in the year – never mind that those invoices were rejected because Plaintiff had already paid for the underlying services.

58. Defendant Jones also had to explain why no money had been forthcoming from the CBP project. He came up with the claim that the payment was delayed because the project was being audited. Not content yet to give up entirely, Defendant Jones further declared that the last task of the SLED development had begun, although he later claimed – not surprisingly – that he could not deliver.

59. By this time, Plaintiff was starting to consider what other options might be available for getting the projects completed. One of the options explored involved Plaintiff buying Defendant's company along with an investor through Merrill Lynch. As part of that process, on or about May 24, 2018, Defendant Jones provided Plaintiff with a one-page summary of Defendant's company. Defendant Jones claimed in the investor summary that he developed the Secure Grid platform, which was just another falsehood among many that Defendant Jones had told about the subject

projects over the years. In fact, the product that Defendant Jones was attempting to pass off as the one he developed for Plaintiff was actually owned and developed by a company named Network Harbor.

60. On or about May 29, 2018, Defendant further pursued the possibility of selling his company to Plaintiff. He sent Plaintiff an email with proposed terms for the purchase. Defendant Jones continued to claim that his company developed and owned the Secure Grid solution and the Secure Gird Smart Card (SLED) solution. Plaintiff rejected the proposal and Defendant Jones later retracted the false statements about Secure Grid when interviewed by Plaintiff and Chris Hellman, the Merrill Lynch analyst.

61. As part of the due diligence process in continuing to explore a possible purchase of Defendant's company, Chris Hellman, the Merrill Lynch analyst, requested the Defendant's company financial information. Defendant Jones would not provide the information and actually began to make accusations that Plaintiff had somehow violated an NDA between the parties.

62. In July of 2018, Renfinity contacted Suh'dutsing directly to inquire about the status of the CBP project. Suh'dutsing informed Renfinity that it had never been part of any Teaming Agreement with Defendant or his company. Based on what Renfinity learned as part of that process, Defendant Jones had in fact visited Suh-dutsing to make a pitch for work, but he was using a product owned by another company. Suh-dutsing told Defendant Jones that his proposed pricing was too high for the CBP project. Notwithstanding the rejection, Defendant told Renfinity that he

had obtained the contract and set about on the elaborate scheme to perpetuate and conceal that fraud.

63. In July of 2018, after Renfinity made its concerns known to Defendant, he promised to provide a complete accounting of the status of all current projects and to arrange a conference call with Suh'dutsing. Defendant provided a purported accounting but he did not follow through on arranging the call for obvious reasons.

64. Around this same time frame, Defendant accused Plaintiff and Chris Hellman of violating the NDA between Plaintiff and Defendant. In essence, Defendant's theory was that Plaintiff had violated the NDA by exposing sensitive information regarding the CBP. In an unsurprising twist that is not difficult to discern, Defendant Jones argued that the alleged NDA violation required Chris Hellman to destroy all evidence he had obtained regarding the CBP pilot.

65. And Defendant's efforts to back his way out of the extensive fraud he committed only continued. On or about July 30, 2018, he advised that he had no new information regarding the CBP pilot payment and actually went so far as to state that the CBP pilot may be in jeopardy due to the alleged breaches of the NDA: "My fear is that the breach caused by Renfinity will cause some delays and potential financial impact." "The breach impacts MSD and its relationship with its customers and standing, which I don't believe Renfinity appreciates the potential damage that has been caused as a result of its inability to honor its commitments under its NDA, both immediate and long term."

66. In early August of 2018, having grown weary of delays and excuses, Plaintiff requested that Defendant Jones demand payment for Plaintiff's Secure Grid solution. Plaintiff provided Defendant Jones with a draft of a proposed demand letter, and still Defendant was not yet finished fighting for time. On or about August 10, 2018, he sent an email stating that "Currently all MSD Enterprises, LLC US government contacts have been called for review under DCAA. This review examines the validity of contract and contractors, accounting and FAR regulations by the requesting DoD and/or other federal agencies. MSD has complied with this request and will immediately advise Renfinity once a response has been received."

67. Defendant Jones followed this false email with one purporting to put Plaintiff on notice of an alleged breach of the NDA. As a remedial measure for these alleged violations of the NDA, Defendant Jones demanded that Plaintiff return and destroy all documents, which, of course, Plaintiff did not do.

68. In late August of 2018, when a collection firm attempted to collect on fees and charges allegedly due and owing to Chris Hellman for the services he provided, Defendant's fraudulent conduct was again confirmed. Services related to the alleged Teaming Agreement were part of that collection effort, and a representative of Suh'dutsing declared that the Teaming Agreement was not an authentic document, as it was "fraudulently signed (neither my legal signature nor my normal initials, which is a separate and distinct matter)" and was not a contract at any rate. Suh'dutsing further declared that there was never a "subcontractor agreement between Suh'dutsing Telecom and MSD Enterprises, LLC and/or MIL-

SPEC ENGINEERING," and that any collection efforts must therefore be directed at those entities, not Suh'dutsing.

69. On or about September 14, 2018, Plaintiff started to push Defendant Jones more forcefully. Plaintiff demanded that Defendant Jones deliver all products Plaintiff had paid him to develop. Defendant Jones responded, effectively denying that he had done anything wrong or that he owed any outstanding obligations to Renfinity. In the weeks that followed, the parties continued to spar in email over the massive fraud Defendant committed, as outlined herein.

70. In subsequent investigation of the relevant facts and witnesses, Plaintiff, acting by and through its attorney on or about January 11, 2019, notified Stafford Mahfouz at JCI of the Defendant's fraudulent activities. Mr. Mahfouz provided the Plaintiff's product demonstration and costing for the Port of Charleston. Mr. Mahfouz stated that Defendant was not and never had been a reseller of JCI and had not developed the Secure Grid solution that Plaintiff paid Defendant to develop. The application Defendant had sold to Plaintiff is a solution that was developed and sold by Network Harbor. Mr. Stafford said Defendant Jones told him that Renee McCown did not want the investors in attendance to know the true facts about the product being demonstrated. Again, Ms. McCown made no such statements or requests. Ms. McCown expected a full and honest presentation of the product.

71. Defendant's fraudulent conduct and activities have caused Renfinity and its investors substantial damages and has resulted in the loss of several potential

business relationships for Renfinity. As a direct and proximate result of Defendant's fraudulent conduct, Renfinity wired Defendant a total of $496,250 as follows:

a. $97,000 on May 5, 2014 for a down payment for Secure Grid development and airfare for Matt Jones ($2,000)

b. $100,000 on January 30, 2015 for Secure Grid application development

c. $65,000 on February 3, 2015 for Secure Grid application development

d. $15,000 on April 10, 2015 for the Secure Grid Smart Access Card (SLED) development

e. $30,000 on October 2, 2015 for completion of payments; payment for a Test Environment, and payment for a Secure Grid video to be shown to potential investors

f. $4,300 on October 29, 2015 for SLED development

g. $20,000 on March 21, 2017 for SLED development

h. $5,000 on April 20, 2017 for SLED development

i. $95,000 on April 25, 2017 for SLED development

j. $4,975 on July 21, 2017 for SLED

k. $25,000 on October 19, 2017 for SLED – Late Payment Penalty

l. $30,000 on October 28, 2017 for drone technology for the CBO Demo

m. $10,000 on December 6, 2017 for drone technology for the CBO Demo

n. $5,000 on January 4, 2018 for drone technology for the CBO Demo

72. Renfinity has also been damaged with respect to Defendant's failure to provide payment of the $1,389,750 pursuant to Purchase Order 20170203 for

completion of the pilot project with the CBP, and Renfinity has incurred operational expenses during the time in which MSD has delayed delivery of the promised system. That amount is estimated at approximately $1.6 million, for which Renfinity is entitled to compensation.

FOR A FIRST CAUSE OF ACTION
(Civil RICO)

73. Plaintiff incorporates all of the forgoing allegations as if fully restated herein.

74. Plaintiff brings this claim pursuant to 18 U.S.C. § 1964(c).

75. Defendant engaged in a scheme or artifice to defraud that involved "racketeering activity." Specifically, 18 U.S.C. § 1961 defines "racketeering activity" to include a whole list of activities, including activities that subject a person to indictment under 18 U.S.C. § 1343 (relating to wire fraud).

76. Sending of emails in connection with a scheme or artifice to defraud constitutes indictable wire fraud under federal criminal law.

77. Defendant here sent numerous emails as part and parcel of his scheme and artifice to defraud Plaintiff, many of which are specified above, thus his activities satisfy the legal requirement that a civil RICO claim be based on a "pattern" of racketeering activities – which only requires two predicate acts.

78. Furthermore, there is sufficient continuity between the predicate acts of fraud alleged herein to sustain this claim. At the very least, the multiple fraudulent communications spanning several years are sufficient to establish closed-ended

continuity. All of the racketeering predicates are related and meet the continuity requirement.

79. As a result of Defendant's violation of the federal RICO statute, Plaintiff has suffered damages as a proximate result of those violations.

80. Under the statute, Plaintiff is entitled to recover treble damages and attorneys' fees.

FOR A SECOND CAUSE OF ACTION
(Fraud)

81. Plaintiff incorporates all of the forgoing allegations as if fully restated herein.

82. Defendant made numerous material misrepresentations, many of which are outlined with specificity in the Facts section above.

83. Defendant also concealed numerous material facts, which are also outlined or described with more specificity in the Facts section above.

84. His actions in making the misrepresentations or omitting the material facts were reasonably calculated to deceive Plaintiff.

85. His actions did in fact deceive Plaintiff.

86. His actions were taken with the intent to deceive Plaintiff.

87. Plaintiff's reliance on Defendant's misrepresentations and fraudulent omissions was reasonable. Indeed, Plaintiff acted reasonably at all times in its interactions with Defendant.

88. As a proximate result of Defendant's fraudulent conduct, Plaintiff has suffered damages in an amount to be proven at trial.

89. Furthermore, Defendant's conduct is such that Plaintiff is entitled to an award of punitive damages.

FOR A THIRD CAUSE OF ACTION
(Breach of Contract)

90. Plaintiff incorporates all of the forgoing allegations as if fully restated herein.

91. Plaintiff and Defendant entered into a valid and binding contract for Defendant to develop the Secure Grid application.

92. Plaintiff fulfilled all of its obligations under the contract.

93. Defendant breached the contract in many ways, including but not limited to failing to perform or deliver on the development of the Secure Grid application, and wrongfully soliciting and accepting payments for work not performed.

94. Defendant ultimately failed to deliver on any of the products he agreed to develop for Plaintiff.

95. As a proximate result of Defendant's breaches of contract, Plaintiff has proximately suffered damages in an amount to be proven at trial.

FOR A FOURTH CAUSE OF ACTION
(Unfair Trade Practices)

96. Plaintiff incorporates all of the forgoing allegations as if fully restated herein.

97. The Defendant committed numerous unfair and deceptive trade practices in making numerous false representations and defrauding Plaintiff out of

nearly a half a million dollars, not to mention other actual damages sustained by Plaintiff.

98. Defendant's unfair and deceptive trade practices were in or affecting commerce.

99. As a proximate result of Defendant's unfair and deceptive trade practices, Plaintiff was injured and suffered damages in an amount to be proven at trial.

100. Pursuant to N.C. Gen. Stat. § 75.1-1, Plaintiff is entitled to an award of attorneys' fees and treble damages.

FOR A FIFTH CAUSE OF ACTION
(Unjust Enrichment)

101. Plaintiff incorporates all of the forgoing allegations as if fully restated herein.

102. Plaintiff conferred certain benefits on Defendant – namely monetary payments in the amount of $496,250.00.

103. Those benefits were not conferred gratuitously, but with the expectation that Defendant would perform his obligations.

104. It would be unjust under the circumstances to allow Defendant to retain the benefit of the funds bestowed upon him by Plaintiff.

FOR A SIXTH CAUSE OF ACTION
(Conversion)

105. Plaintiff incorporates all of the forgoing allegations as if fully restated herein.

106. Plaintiff was and is the proper owner of the funds transferred to Defendant by virtue of Defendant's fraudulent actions.

107. By his actions, Defendant has wrongfully converted those funds and interfered with Plaintiff's ownership interest therein, obtaining and exercising improper and unlawful dominion and control over those funds.

108. As a proximate result of Defendant's tortious conduct, Plaintiff suffered damages in an amount to be proven at trial.

109. Furthermore, Defendant's actions are such that Plaintiff is entitled to an award of punitive damages under N.C. Gen. Stat. § 1D-15.

PRAYER FOR RELIEF

110. As a result of the forgoing claims and allegations, Plaintiff respectfully requests that the Court enter judgment in Plaintiff's favor for (1) actual damages; (2) costs and expenses; (3) attorneys' fees; (4) any applicable statutory multiples of damages, including but not limited to treble damages under the federal civil RICO statute or the North Carolina UTPA; and (5) punitive damages where appropriate. Plaintiff further requests that the Court grant it all other relief to which it is legally entitled and which the Court deems just and proper. Plaintiff demands trial by jury for all issues so triable.

(signature page follows)

This the 30 day of July, 2020.

BONDURANT LITIGATION

s/ Joel M. Bondurant, Jr.
JOEL M. BONDURANT, JR.
Attorney for Renfinity, Inc.,
NC Bar No. 29621
13850 Ballantyne Corp. Pl., Ste. 500
Charlotte, NC 28277
(704) 897-0490 (ph); (704) 559-3379 (fax)
joel@bondurantlawfirm.com